UNITED STATES DISTRICT
COURT DISTRICT OF MINNESOTA
Criminal No. 15-CR-11 (PJS/SER)

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	**GOVERNMENT'S POSITION**
	)	**WITH RESPECT TO SENTENCING**
v.	)	
	)	
MAXIM SENAKH,	)	
	)	
Defendant.	)	

The United States of America, by and through its attorneys Gregory G. Brooker, Acting United States Attorney for the District of Minnesota, Timothy Rank, Assistant United States Attorney, Benjamin Fitzpatrick, Senior Counsel, Criminal Division, and Aaron Cooper, Senior Counsel, Criminal Division, hereby submits its position with respect to the sentencing of defendant Maxim Senakh. On March 28, 2017, the defendant pled guilty to one count of conspiracy to violate the Computer Fraud and Abuse Act and to commit wire fraud, in violation of 18 U.S.C. § 371. PSR ¶2. The Presentence Investigation Report ("PSR") calculated the defendant's total offense level to be 23 and his criminal history category to be I, resulting in a Sentencing Guidelines range of 46 to 57 months of imprisonment. *Id*. at ¶62. This range aligns with the range contemplated in the parties' plea agreement. *Id*. at ¶64. For the reasons set forth below, the Government believes that a sentence at the top of the applicable Guidelines range is appropriate. The Government respectfully requests that the Court impose a sentence of 54 months of imprisonment.

FACTUAL BACKGROUND

Since at least 2008, Senakh conspired with others to install malicious computer software ("malware") onto thousands of computer servers located throughout the world, and has directly and substantially assisted with exploiting this malware to defraud victim entities of significant quantities of money. *Id*. at ¶6**.** According to admissions made in the parties' plea agreement, the malware, which is known as Ebury, harvested log-on credentials from infected computer servers, allowing Senakh and his co-conspirators to create and operate a network of thousands of infected servers throughout the world, known as a botnet. *Id*. at ¶¶6, 7.

Senakh was integrally involved in creating and maintaining sophisticated infrastructure that supported the Ebury botnet and the conspiracy's fraudulent schemes. *Id*. at ¶¶11, 12. Specifically, he and his co-conspirators created accounts at domain registration companies that members of the conspiracy used to register domain names for "Command and Control" servers, *i.e.*, the servers they used to direct their botnet traffic. These domain names were also used for servers that received the stolen credentials from Ebury-infected computers. *Id*. Senakh also created a key Googlemail account that he subsequently transferred to members of the conspiracy, along with a domain registration account, to use in registering additional domains. *Id*. at ¶12. He knew these domains would support the Ebury botnet and that he and other members of the conspiracy would benefit financially from them. *Id*. at ¶13.

Senakh and his co-conspirators used the Ebury botnet to generate and redirect Internet traffic in furtherance of various click-fraud and spam e-mail schemes, which fraudulently generated millions of dollars in illicit revenue. *Id.* at ¶9. To perpetrate their click-fraud scheme, Senakh and his co-conspirators installed additional malware on Ebury-infected web servers. *Id.* When Internet users visited websites hosted on those infected servers, this malware automatically re-directed those users to websites for entities that had hired Senakh or members of the conspiracy as advertising affiliates. *Id.* This redirected traffic was programmed by members of the conspiracy to look like legitimate traffic of users who had "clicked" on an online advertisement Senakh or others had placed, when in fact they had been involuntarily redirected from another website. *Id.* The entities would pay Senakh and members of the conspiracy based on the amount of traffic generated by the conspiracy.

Members of the conspiracy also exploited the Ebury botnet to send tens of millions, if not more, spam e-mail messages. PSR ¶10. The purpose of these messages was to entice recipients to click on links that would route the recipients through Ebury-infected servers to websites of advertisers. *Id.*

Senakh actively participated in, and generated revenue from, the click-fraud scheme, and knew about the spam e-mail scheme. PSR ¶13. For example, he monetized the Ebury botnet by knowingly exploiting traffic he knew had been redirected from websites hosted on Ebury infected servers, and directed it to adult websites with which he had an advertising relationship. *Id.* One such website was Adult Friend Finder ("AFF"). Senakh defrauded AFF, which paid him for illegitimate traffic. AFF paid Senakh and his co-conspirators $228,018.56. *Id.* at ¶¶14-16.

ARGUMENT

It is the position of the Government that the appropriate sentence for the defendant is 54 months of imprisonment. A full consideration of the factors set forth in Section 3553(a) compels the Government to seek this sentence, including in particular the nature and circumstances of the offense and the need to provide adequate deterrence to the defendant and other cybercriminals.

In *Gall v. United States*, 552 U.S. 38 (2007), the Supreme Court set forth the appropriate sentencing methodology: the district court calculates the advisory Guideline range and, after hearing from both parties, considers the 18 U.S.C. § 3553(a) factors to determine an appropriate sentence. 552 U.S. at 49-50; *United States v. Ruvalcava-Perez*, 561 F.3d 883, 886 (8th Cir. 2009) ("In sentencing a defendant, the district court should first determine the appropriate Guidelines range, then evaluate whether a traditional departure is warranted, and finally decide whether or not to impose a guideline sentence after considering all of the § 3553(a) sentencing factors").

The district court may not assume that the Guidelines range is reasonable, but instead "must make an individualized assessment based on the facts presented." *Id*. at 50. If the court determines that a sentence outside the Guidelines is called for, it "must consider the extent of the deviation and ensure that the justification is sufficiently compelling to support the degree of the variance." *Id*. Section 3553(a) requires the Court to analyze a number of factors, including, "the nature and circumstances of the offense," the history and characteristics of the defendant," "the need for the sentence to reflect the seriousness of the offense," "the need for deterrence," "the need to protect the public from further crimes of the defendant," and "the need to avoid unwarranted disparities." 18 U.S.C. § 3553(a).

1. Nature and Circumstances of the Offense.

The nature and circumstances of this offense merit a significant sentence at the high end of the sentencing guidelines range. The Ebury Botnet is highly-sophisticated and has infected tens of thousands of computers in Minnesota and around the world. According to a 2014 report on the Ebury Botnet by the cybersecurity firm ESET:

- In the two years preceding publication of the report, more than 25,000 unique servers had been compromised;
- On average, more than 35 million spam messages were sent ***daily***;
- More than 700 web servers actively redirected visitors to malicious content; and,
- Over 500,000 visitors to legitimate websites hosted on servers compromised by Ebury are redirected to additional "exploit kits" every day.

See Operation Windigo, available at https://www.welivesecurity.com/wp-content/uploads/2014/03/operation_windigo.pdf. Operating this botnet required registering and maintaining hundreds, possibly thousands, of web domains—often created with fake identifying information to hide the conspirators' true identities—to control the botnet, prevent it from being detected and blocked by Internet service providers, and direct the Internet traffic it created. Malware installed by members of the conspiracy on victims' computers and servers was specially programmed to and did steal credentials and other personal information. Senakh and his co-conspirators exploited this illicitly-constructed global infrastructure over a period of years to defraud legitimate companies interested in advertising their products and services to customers. In short, this was a scheme to get rich at others' expense, carried out in a way to avoid attribution.

Sophisticated criminal operations like this conspiracy represent a significant threat to public safety. Botnets have been used to seize control of victims' computer systems, steal highly personal information and money, commit fraud, and disseminate and control ransomware and other malware. Click-fraud and mass spam e-mail schemes operate to undermine legitimate businesses and clog a vital means of communication with unsolicited, unwanted, and bandwidth-consuming communications; they are also used to spread malware. As our society becomes more reliant on computers, networks, and Internet operations, the need to protect those same networks and computers, and especially the personal data contained on them, from unauthorized access and expropriation increases. Imposing a serious punishment would reflect society's substantial interest in safeguarding our computers and systems from the kind of widespread, unlawful activity that Senakh directly and willfully supported for years. The sentence should resonate with Senakh and the many current and would-be hackers who believe cybercrime to be a low-risk, high-reward proposition.

A sentence of 54 months' imprisonment is consistent with the significant punishments that have been imposed in other cases involving criminal use of botnets and malware. In one case, two hackers who developed the "SpyEye" malware received sentences of 9 and 15 years. *See* Judgment and Commitment, United States v. Panin, No. 11-CR-557 (N.D. Ga. Apr. 25, 2016), ECF Nos. 191-192. The malware was designed to automate the theft of personal and financial information from victims' systems by allowing criminals to remotely control infected computers using command and control servers.

Hundreds of millions of dollars in losses to financial institutions worldwide were attributed to SpyEye. While this figure eclipses the losses attributed to Ebury, the severity of that sentence clearly demonstrates the importance courts have placed on sentencing defendants in cases involving the use of widespread malware to perpetuate criminal enterprises. In another case involving exploitation of malware, the owner of an organization that sold and distributed sophisticated malware to thousands of people in more than 100 countries, and which was used to infect more than half a million computers worldwide, was sentenced to 57 months in prison. *See* Judgment & Transcript, United States v. Yucel, No. 13-cr-834 (SDNY June 24, 2015), ECF Nos. 54-55.

2. History and Characteristics of Defendant.

Senakh pled guilty to supporting a massive criminal enterprise that has operated for nearly a decade—a serious crime which his punishment should reflect. As the evidence would have shown had this gone to trial, Senakh was directly involved in creating infrastructure that allowed the Ebury botnet to operate on systems owned by innocent victims throughout the world, and exploited the resulting traffic for his own financial gain. Still, the full extent of Senakh's involvement remains unknown and unknowable. When he was arrested by Finnish authorities, he was carrying several electronic devices, including an encrypted, 120 gigabyte hard drive to which the government has not successfully gained access – in part because Senakh has refused requests to provide the password to decrypt the drive. Given the sophistication of the encryption utilized by Senakh, it stands to reason that the hard drive contains *further* evidence of Senakh's involvement in this criminal enterprise, or other criminal activity. Accordingly, notwithstanding the fact that his criminal history falls at the low end of the scale, it is clear that Senakh's extensive involvement in the Ebury botnet is not an aberrant, one-off mistake of an otherwise law-abiding individual, but the consistent, conscious and willful behavior of someone intent on ensuring that the Ebury botnet would grow and succeed.

It also merits noting that Senakh's low criminal history category reflects the challenges law enforcement faces with attributing computer crimes to specific defendants, as well as the difficulties of apprehending foreign-based defendants like Senakh whose governments generally do not extradite their citizens to the United States. Indeed, once released from prison, Senakh will likely be immediately deported back to Russia, where he will be free to return to engaging in criminal activity from outside the effective reach of United States law enforcement authorities. He will not benefit from oversight provided by supervised release, nor will the community receive the public safety benefit from such oversight of Senakh and his activities. Imposing a significant term of imprisonment will apply the greatest incentive on Senakh not to return to criminal activity and will best protect public safety given the likely inability to monitor his activity post-incarceration.

3. The Need for the Sentence Imposed to Reflect the Seriousness of the Offense, to Promote Respect for the Law, and to Provide Just Punishment for the Offense.

A sentence at the high end of the Guidelines range would properly reflect the seriousness with which society takes computer hacking crimes, foster greater respect for U.S. law by foreign criminals, and provide a just punishment for the offense. As noted above, crimes involving installing malware on victims' computers present unique challenges. Use of sophisticated technologies make attributing these crimes, when they are even discovered, to particular individuals incredibly difficult. In addition, these crimes are often global in scope, meaning that even if law enforcement is able to identify those responsible, they too often reside outside the reach of law enforcement. Here, Senakh is a citizen of Russia, a nation that is not responsive to requests by U.S. law enforcement. The Government was only able to bring Senakh to justice because he traveled from Russia to a country that would respect a request to arrest him and extradite him to face trial here in the United States.

It is appropriate to send a clear signal that criminals should not believe their online activities are beyond the reach of punishment by the United States' criminal justice system simply because they reside in a different country. Further, these challenges to attributing and prosecuting criminals such as Senakh make it all the more important to send a strong message when a criminal like Senakh is caught and brought to justice.

4. The Need for the Sentence to Afford Adequate Deterrence to Criminal Conduct, and the Need for the Sentence Imposed to Protect the Public from Future Crimes of this Defendant.

In this case, there is need for both individualized and general deterrence. Individualized deterrence is that which discourages a defendant from ever committing such a crime again. As noted above, Senakh is likely to return to Russia soon after his term of incarceration ends. A serious sentence represents the best tool to motivate Senakh to apply his considerable technical abilities toward legitimate purposes.

A sentence at the high range of the sentencing guidelines range would also serve as an important general deterrent. General deterrence is the public response necessary to deter other people from committing similar crimes. "Congress specifically made general deterrence an appropriate consideration … and we have described it as 'one of the key purposes of sentencing.'" *Ferguson v. United States*, 623 F.3d 627, 632 (8th Cir. 2010) (quoting *United States v. Medearis*, 451 F.3d 918, 920 (8th Cir. 2006)). As noted above, given the difficulties law enforcement faces with attributing computer crimes and apprehending those responsible, a significant punishment in this case would send a clear deterrent message to others engaged in cyber-crime, including by highlighting the travel risks attendant to engaging in criminal activity from countries that are not responsive to extradition requests from the United States.

CONCLUSION

For the reasons set forth above, the Government respectfully asks the Court to sentence the defendant to 54 months' imprisonment.

Dated: July 13, 2017

Respectfully Submitted,

Gregory G. Brooker
Acting United States Attorney

s/ Timothy Rank
BY: Timothy Rank
Assistant U.S. Attorney